WHAT IS CLAIMED IS:

1. A method of revoking a device, the method comprising:
receiving a certificate from the device, the certificate including one or more of fields, at least one of the fields holding a signature;
attempting to verify the signature;
receiving a revocation list from a source, the revocation list identifying one or more data on the certificate as valid or invalid, the data including at least one of the fields of the certificate; and
if one of one or more signatures identified unsuccessfully verified and one or more data is identified as invalid, preventing the transmission of a session key to the device, the session key being required to establish a secure communication channel.

2. The method of claim 1 wherein the revocation list is evaluated upon file access.

3. The method of claim 2 wherein the revocation list is stored upon file creation.

4. The method of claim 1 wherein each file has one revocation list, a plurality of files with a plurality of revocation lists having duplicative entries.

5. The method of claim 4 wherein the duplicative entries among a plurality of revocation lists are limited by centrally storing the details and providing each file with a list of identifiers or pointers that reference a location of complete details regarding revocation information.

6. The method of claim 5 wherein the revocation information may be stored by revocation nodes and the revocation list associated with a file may be stored as a list of revocation node identifiers.

7. The method of claim 6 wherein each revocation node consists of a list of clauses and a rule for combining the clauses for determining the evaluation for the node.

8. The method of claim 7 wherein the revocation results are finalized by one of get play key, play, record, copy, open, close, create, get metadata and set metadata.

9. The method of claim 1 wherein the revocation list is stored on media along with the file.

10. The method of claim 1 wherein the revocation list is copied onto each device.

11. The method of claim 1 wherein the revocation list is maintained by a server such that content rendering devices communicating with a server receive updated revocation lists directly to the device.

12. The method of claim 1 wherein a plurality of revocation lists are stored on media on a file-by-file basis, such that one or more files on the media may have a revocation list associated with the file.

13. The method of claim 12 wherein the revocation list is accessed during one of a file access process and a combination of both an authentication and a file access process.

14. The method of claim 1 wherein the revocation list includes a poison pill that prevents a content rendering device from operating.

15. The method of claim 1 wherein the revocation list is updated when the content rendering device is connected to a server.

16. The method of claim 1 wherein revocation of a content rendering device includes at least revocation of one or more public keys, the revocation of a public key revoking any corresponding signature.

17. The method of claim 1 wherein the revocation list is maintained as an object within the file system on the media with a distinct handle.

18. The method of claim 1 wherein the revocation information is centrally located.

19. The method of claim 1 wherein the source is one of a portable medium and firmware.

20. The method of claim 1 wherein the information as to whether certificates and/or public keys have been revoked is stamped on the media.

21. The method of claim 1 wherein the device is one of an engine, a component that embeds an engine, a third party digital rights management protocol, an application running in an open computing environment, and a clearinghouse server, the certificate identifying one or more secure application programming interfaces (APIs) for which an application operable with the device may have access.

22. The method of claim 1 wherein the certificate is signed by a private key assigned according to a class of device, the class of device including engines, components embedding an engine with no external digital input/output port, components embedding an engine with digital input/output ports, and host applications not embedding an engine.

23. The method of claim 1 wherein the data in the certificate specifies one or more of a product category, a product line, a model, a revision and a serial number of the device.

24. The method of claim 23 wherein source validation data is compared with the data on the certificate to identify as invalid one or more of the product category, the product line, the model, the revision and the serial number of the host.

25. The method of claim 24 wherein the certificate includes one or more of the following fields: certifying authority identifier, version, certifying authority public key, certifying authority public key identifier, exposed methods, company, model identifier, revision, metadata identifier, host signature public key, certifying authority signature, serial number, protocol key and host signature, wherein the certifying authority signature verifies one or more of the fields in the certificate and the host signature verifies one or more of the fields in the certificate.

26. The method of claim 1 wherein the certificate enables an entity receiving the certificate to control quality of the device by invalidating devices that are false or have latent defects.

27. The method of claim 25 wherein the certificate further includes fields provided by a device manufacturer, including the device public key, wherein the device public key is signed by a private key.

28. The method of claim 25 wherein one or more of the product category, the product line, the model, the revision and the serial number of the host are provided to a certificate creator after the host passes a qualification procedure.

29. The method of claim 1 wherein the certificate specifies one or more certificate classes, the certificate classes providing a set of methods that may be exposed after the transmitting the session key.

30. The method of claim 29 wherein the set of methods includes digital rights management (DRM) methods, copy, record, play, read secure metadata, write secure metadata, and unlock, the methods operable according to a type of the device.

31. The method of claim 30 wherein:

the unlock method is associated with a clearinghouse server;

the copy method is associated with one of an engine and a first DRM application operable with a second DRM application; and

the import method is associated with one or more of a player, a mastering tool, a kiosk, and a clearinghouse server.

32. The method of claim 1 wherein each of the fields hold 326-bit values for 163-bit elliptic curve cryptography.

33. An apparatus for revoking a host, the apparatus comprising:

means for receiving a certificate from a host, the certificate including a plurality of fields including a field holding a protocol public key signed by a certifying authority;

means for verifying signatures on the certificate, the verifying including:

verifying the certifying authority signature using the protocol public key; and

verifying a host signature using a host public key on the certificate; and

means for receiving validation data from a source, the validation data identifying one or more data on the certificate as valid or invalid according to a revocation list; and

means for preventing the transmission of a session key to the host to establish a secure communication channel if the signatures are invalid.

34. An engine configured to revoke a host, the engine comprising:
a block configured to receive a certificate from a host, the certificate including a plurality of fields including a field holding a protocol public key signed by a certifying authority;
a block configured to verify signatures on the certificate, the verifying including:
verifying the certifying authority signature using the protocol public key; and
verifying a host signature using a host public key on the certificate; and
a block configured to receive validation data from a source, the validation data identifying one or more data on the certificate as valid or invalid according to a revocation list; and
a block configured to preventing the transmission of a session key to the host to establish a secure communication channel if the signatures are invalid.

35. A computer program product, the computer program product comprising:
signal bearing media bearing digital information adapted to be operable with a firmware), the digital information including programming including:
a block configured to receive a certificate from a host, the certificate including a plurality of fields including a field holding a protocol public key signed by a certifying authority;
a block configured to verify signatures on the certificate, the verifying including:
verifying the certifying authority signature using the protocol public key; and
verifying a host signature using a host public key on the certificate; and
a block configured to receive validation data from a source, the validation data identifying one or more data on the certificate as valid or invalid according to a revocation list; and
a block configured to preventing the transmission of a session key to the host to establish a secure communication channel if the signatures are invalid.